POLICY 4.00 USER ACCESS & ACCEPTABLE USE

Information resource asset access privileges will be limited to the minimum required for an individual to successfully complete his/her job duties.

PURPOSE:

To ensure satisfactory segregation of duties and to support transaction level accountability.

REFERENCE:

Tennessee Code Annotated, Section 4-3-5501, effective May 10, 1994.
"State of Tennessee Acceptable Use Policy"
(http://www.state.tn.us/training/CA/net_use_policy.html)
"User Agreement Acknowledgement"
(http://www.state.tn.us/training/CA/net_use_agmnt.html).

OBJECTIVES:

1. Ensure individual awareness and compliance with the "State of Tennessee Acceptable Use Policy" reflected by a signed "User Agreement Acknowledgement". Continued awareness and compliance shall be evidenced by an annual individual "User Agreement Acknowledgement" renewal.
2. Ensure information technology resource logical access privileges are restricted to those within the scope of their authority.
3. Promote individual accountability evidenced by an information access audit trail.
4. Promote individual accountability through access role authorities and permissions.
5. Protect critical state information resource systems, application, and data from unauthorized use, misuse, or destruction.
6. Promote the safeguarding of information technology resources in a cost effective manner such that the cost of security is commensurate with the value and sensitivity of the resources.

SCOPE:

The scope includes access to any State of Tennessee information technology resource and related component including hardware, software, data, documentation, and reports, as well as individual accountability for acceptable use of email and the Internet.

IMPLEMENTATION:

Office for Information Resources (OIR)

1. Develop, implement and maintain standards for acceptable information resource access.
2. Assign responsibility for monitoring and enforcing logical access.
3. Maintain audit trails for administrative access to OIR managed information technology resources.

Agency

1. Refrain from implementing agency procedures, processes or practices that would expose networked information resources to unnecessary or unauthorized risks.
2. Assign responsibility for monitoring and enforcing actual local access.
3. Maintain audit trails for administrative access to agency managed information technology resources.

Individual Users/Clients

1. Act within the scope of their approved information access authority.
2. Refrain from behaviors that could compromise the integrity of information technology resources including, but not limited to, behaviors reflected in the "State of Tennessee Acceptable Use Policy".